暗号から数論へ : 代数曲線に関するいくつかのアルゴリズム (解析的整数論とその周辺 : 近似と漸近的手法を通して見た数論)

AUTHOR(S):

内山, 成憲; 内田, 幸寛

CITATION:

内山, 成憲 ...[et al]. 暗号から数論へ : 代数曲線に関するいくつかのアルゴリズム (解析的整数論とその周辺 : 近似と漸近的手法を通して見た数論). 数理解析研究所講究録 2014, 1874: 32-44

ISSUE DATE:

2014-01

URL:

http://hdl.handle.net/2433/195546

数理解析研究所講究録
第1874巻 2014年 32-44

暗号から数論へ – 代数曲線に関するいくつかのアルゴリズム –

From cryptography to number theory – some algorithms on algebraic curves –

首都大学東京・大学院理工学研究科・数理情報科学専攻
内山 成憲，内田 幸寛
Shigenori UCHIYAMA, Yukihiro UCHIDA
Department of Mathematics and Information Sciences
Graduate School of Science and Engineering
Tokyo Metropolitan University
uchiyama-shigenori@tmu.ac.jp, yuchida@tmu.ac.jp

1 はじめに

暗号と数論との明示的な関係は，1970年代に提案され現在世界中で最も広く使用されている公開鍵暗号方式であるRSA暗号の提案まで遡ることが出来る．RSA暗号は十分大きなサイズの合成数の素因数分解問題の計算量的な困難さにその安全性の根拠をおいているが，その後，素因数分解問題と同様の計算量的困難さを持つと期待される有限体上の離散対数問題等，いくつかの数論的な問題の困難さに基づく実用的な暗号方式が提案されてきた．このように，この30年程の間，暗号理論は数論，特に計算数論と密接な関係を保ちながら発展してきたとも言えよう．特に特筆すべきは代数曲線に関するアルゴリズム研究の発展である．これは，1980年代にKoblitzとMillerにより独立に提案された楕円曲線暗号の提案により明示的になったと言えよう．ここでは，楕円曲線暗号の安全性評価研究の際に利用されたことで注目され，その後IDベース暗号に代表されるペアリング暗号と呼ばれる一連の暗号方式の研究へとつながった

代数曲線上のペアリングに関連するいくつかのアルゴリズムについて述べる.

代数曲線上にはWeilペアリングをはじめ,様々なペアリングが定義されているが,計算速度等の観点から,Tate-Lichtenbaumペアリング(単にTateペアリングとも呼ぶ)やその変種がよく用いられている.このペアリングは,まずTate [14]によって,Abel多様体上のペアリングとして定義された.Lichtenbaum [6]は,Abel多様体がある代数曲線のJacobi多様体である場合に,Tateの定義したペアリングを曲線の言葉で書き表した.Frey-Rück [4]は,彼らの結果を有限体上定義された代数曲線に対して適用し,Jacobi多様体上の離散対数問題に応用した.

Tate-Lichtenbaumペアリングの計算には,Millerのアルゴリズムがよく用いられてきた(cf. [4, 7, 8]).2007年,Stange [11]は楕円曲線のTateペアリングを計算する新しいアルゴリズムを提案した.このアルゴリズムでは,elliptic divisibility sequence (EDS)の一般化としてStangeによって定義された,elliptic netが用いられる.

本稿では,elliptic netを超楕円曲線に一般化してhyperelliptic netを定義し,これを用いて超楕円曲線上のTate-Lichtenbaumペアリングを書き表す公式を与える.また,種数2の超楕円曲線に対して,hyperelliptic netが満たす漸化式に基づくTate-Lichtenbaumペアリングの計算アルゴリズムを述べる.本稿の内容は[15]に基づく.証明は省略したので,[15]を参照していただきたい.

2 Elliptic net

本節ではStangeの定義したelliptic netについて述べる.詳細については,[11, 12]を参照していただきたい.Elliptic netはEDSを一般化したものであるので,まずEDSについて述べる.

定義 1 (M. Ward [16]). 整数列 $\{h_n\}_{n\geq 0}$ が,**elliptic divisibility sequence** (EDS) であるとは,

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}{h_n}^2 - h_{n+1}h_{n-1}{h_m}^2$$

がすべての $m \geq n \geq 1$ に対して成り立ち,n が m を割り切るならば h_n が h_m を割り切ることをいう.

Ward は，(適当な条件を満たす) EDS が楕円曲線とその上の 1 点の組と対応することを証明した (cf. [16, Theorem 12.1]).

Stange は，EDS を一般化して，elliptic net を次のように定義した.

定義 2 (Stange [11]). A を有限生成自由 Abel 群，R を整域とする．写像 $W\colon A \to R$ が **elliptic net** であるとは，すべての $p, q, r, s \in A$ に対して次の式が成り立つことをいう.

$$\begin{aligned} &W(p+q+s)W(p-q)W(r+s)W(r) \\ &\quad + W(q+r+s)W(q-r)W(p+s)W(p) \\ &\quad + W(r+p+s)W(r-p)W(q+s)W(q) = 0. \end{aligned}$$

前に定義した EDS $\{h_n\}_{n\geq 0}$ を $h_{-n} = -h_n$ によって $\mathbb{Z}$ 上の数列に拡張すると，写像 $W\colon \mathbb{Z} \to \mathbb{Z}; n \mapsto h_n$ は elliptic net になることが確かめられる.

EDS と同様に，elliptic net も楕円曲線と対応する．その対応を述べるために，楕円曲線 E，自然数 n，$\boldsymbol{v} \in \mathbb{Z}^n$ に対し，E^n 上の有理関数 $\Psi_{\boldsymbol{v}}$ を構成する.

まず，E が複素数体上定義されている場合を考える．このとき，$\mathbb{C}$ 内の格子 Λ と同型 $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ が存在する．格子 Λ に対応する Weierstrass の σ 関数を

$$\sigma(u) = u \prod_{\omega \in \Lambda \setminus \{0\}} \left(1 - \frac{u}{\omega}\right) \exp\left(\frac{u}{\omega} + \frac{u^2}{2\omega^2}\right)$$

で定義する．$\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{Z}^n$ に対し，$\mathbb{C}^n$ 上の有理型関数 $\Psi_{\boldsymbol{v}}$ を

$$\Psi_{\boldsymbol{v}}(u_1, \ldots, u_n) = \frac{\sigma(v_1 u_1 + \cdots + v_n u_n)}{\displaystyle\prod_{i=1}^{n} \sigma(u_i)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j} \prod_{1 \leq i < j \leq n} \sigma(u_i + u_j)^{v_i v_j}}$$

で定義する．$\Psi_{\boldsymbol{v}}$ は各変数に対して Λ を周期に持つので，$\Psi_{\boldsymbol{v}}$ を E^n 上の有理関数とみなすことができる．そこで，$P_1, \ldots, P_n \in E(\mathbb{C})$ が $u_1, \ldots, u_n \in \mathbb{C}$ に対応するとき，$\Psi_{\boldsymbol{v}}(P_1, \ldots, P_n) = \Psi_{\boldsymbol{v}}(u_1, \ldots, u_n)$ と定める.

楕円曲線 E が (標数 0 とは限らない) 一般の体 K 上で定義されている場合も，E^n 上の有理関数 $\Psi_{\boldsymbol{v}}$ で同様の性質を持つものが定義できる.

$P_1, \ldots, P_n \in E(K)$ として，$\boldsymbol{P} = (P_1, \ldots, P_n)$ とおく．今定義した $\Psi_{\boldsymbol{v}}$ を用いて，写像 $W_{\boldsymbol{P}}\colon \mathbb{Z}^n \to K$ を

$$W_{\boldsymbol{P}}(\boldsymbol{v}) = \Psi_{\boldsymbol{v}}(\boldsymbol{P})$$

で定義する.

定理 3 (Stange [11, Theorem 4]). $W_{\boldsymbol{P}}$ は elliptic net である.

この $W_{\boldsymbol{P}}$ を E と $\boldsymbol{P}$ に対応する elliptic net という. 逆に, elliptic net $W\colon \mathbb{Z}^n \to K$ が与えられたとき, W がある条件を満たせば, K 上定義された楕円曲線 E と n 点 $P_1, \ldots, P_n \in E(K)$ が存在して, $W = W_{\boldsymbol{P}}$ となることが示される (cf. [12, Theorem 6.7]).

3 楕円曲線上の Tate ペアリング

本節では, Stange [11] で与えられた, 楕円曲線上の Tate ペアリングを elliptic net によって表す公式について述べる.

$\mathbb{F}_q$ を q 個の元を持つ有限体, $\overline{\mathbb{F}}_q$ をその代数閉包とする. E を $\mathbb{F}_q$ 上定義された楕円曲線として, E の加法の単位元を O で表す. m を $q-1$ の正の約数, $E(\mathbb{F}_q)[m] = \{P \in E(\mathbb{F}_q) \mid [m]P = O\}$ とする.

E 上の Tate ペアリングは, 写像

$$\tau_m\colon E(\mathbb{F}_q)[m] \times E(\mathbb{F}_q)/mE(\mathbb{F}_q) \to \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^m$$

であり, 次のように定義される. $P \in E(\mathbb{F}_q)[m]$ とする. $[m]P = O$ だから, $\mathrm{div}(f_P) = m(P) - m(O)$ となる, $\mathbb{F}_q$ 上定義された E 上の有理関数 f_P が存在する. $Q \in E(\mathbb{F}_q)$ に対し, 線形同値 $(Q) - (O) \sim \sum_{i=1}^r n_i(Q_i)$ が成り立つような $n_1, \ldots, n_r \in \mathbb{Z}$, $Q_1, \ldots, Q_r \in E(\overline{\mathbb{F}}_q)$ $(Q_i \neq P, O)$ を選ぶ. ここで, 右辺の因子は $\mathbb{F}_q$ 上定義されているようにする. このとき,

$$\tau_m(P, Q) = \prod_{i=1}^r f_P(Q_i)^{n_i} \bmod (\mathbb{F}_q^\times)^m$$

と定義する. (左辺は正確には $\tau_m(P, Q \bmod mE(\mathbb{F}_q))$ であるが, 省略して $\tau_m(P, Q)$ と表す. 以下でも同様の省略を行う.)

Stange は, elliptic net を用いて Tate ペアリングを表示する公式を与えた.

定理 4 (Stange [11, Corollary 1]). $P \in E(\mathbb{F}_q)[m]$, $Q \in E(\mathbb{F}_q)$, $P, Q, P + Q \neq O$ とする. このとき次の式が成り立つ.

$$\tau_m(P, Q) = \frac{W_{P,Q}(m+1, 1) W_{P,Q}(1, 0)}{W_{P,Q}(m+1, 0) W_{P,Q}(1, 1)} \bmod (\mathbb{F}_q^\times)^m.$$

また, Stange は, この公式を用いて Tate ペアリングを計算するアルゴリズムを与えた.

以下では, Stange の結果を超楕円曲線に拡張する.

4 Hyperelliptic net

本節では hyperelliptic net を定義し，その性質について述べる．詳細については，[15, §§ 3–4] を参照していただきたい．Elliptic net は漸化式で定義されたが，hyperelliptic net については，先に超楕円曲線をもとに写像を定義し，それが満たす漸化式を証明する．

C を方程式

$$y^2 + (b_g x^g + \cdots + b_0)y = x^{2g+1} + a_{2g}x^{2g} + \cdots + a_0$$

で定まる体 K 上定義された種数 g の超楕円曲線とする．C のただ 1 つの無限遠点を ∞ で表す．

J を C の Jacobi 多様体とする．J は g 次元 Abel 多様体である．C の K 上定義された次数 0 の因子類全体がなす群を $\mathrm{Pic}^0(C)$ とすれば，群同型 $\lambda\colon \mathrm{Pic}^0(C) \to J(K)$ が存在する．J のテータ因子 Θ を

$$\Theta = \left\{ \lambda\left(\sum_{i=1}^{g-1}(P_i) - (g-1)(\infty)\right) \middle| P_1, \ldots, P_{g-1} \in C \right\}$$

で定める．

楕円曲線の場合と同様に，まず複素数体上で考える．超楕円曲線 C が $\mathbb{C}$ 上定義されているとする．このとき，$\mathbb{C}^g$ 内の格子 Λ と，同型 $J(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$ が存在する．

Weierstrass の σ 関数の一般化として，超楕円 σ 関数 $\sigma\colon \mathbb{C}^g \to \mathbb{C}$ が定義されている．σ は整関数である．また，$\sigma(u) = 0$ となるのは $u \bmod \Lambda$ がテータ因子 Θ 上の点に対応するときであり，そのときに限る．超楕円 σ 関数の定義やより詳しい性質については，[2, 9] やその中で挙げられている文献を参照していただきたい．

n を自然数とし，$\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{Z}^n$ とする．$(\mathbb{C}^g)^n$ 上の有理型関数 $\Phi_{\boldsymbol{v}}$ を次の式で定義する．

$$\Phi_{\boldsymbol{v}}(u^{(1)}, \ldots, u^{(n)}) = \frac{\sigma(v_1u^{(1)} + \cdots + v_nu^{(n)})}{\prod_{i=1}^{n} \sigma(u^{(i)})^{2v_i^2 - \sum_{j=1}^{n} v_iv_j} \prod_{1 \le i < j \le n} \sigma(u^{(i)} + u^{(j)})^{v_iv_j}}.$$

超楕円 σ 関数の擬周期性から，$\Phi_{\boldsymbol{v}}$ は各変数について Λ を周期に持つ．よって，$\Phi_{\boldsymbol{v}}$ を J^n 上の有理関数とみなすことができる．$P_1, \ldots, P_n \in J(\mathbb{C})$ が $u^{(1)}, \ldots, u^{(n)} \in \mathbb{C}^g$ に対応するとき，$\Phi_{\boldsymbol{v}}(P_1, \ldots, P_n) = \Phi_{\boldsymbol{v}}(u_1, \ldots, u_n)$ と定める．

$\Phi_{\boldsymbol{v}}$ が満たす性質をいくつか述べる．

命題 5. 任意の $\boldsymbol{v} \in \mathbb{Z}^n$ に対し，

$$\Phi_{-\boldsymbol{v}} = \begin{cases} -\Phi_{\boldsymbol{v}} & (g \equiv 1,2 \pmod 4), \\ \Phi_{\boldsymbol{v}} & (g \equiv 0,3 \pmod 4). \end{cases}$$

$\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ を $\mathbb{Z}^n$ の標準基底とする．

命題 6. $\boldsymbol{v} \in \mathbb{Z}^n$ とする．

1. 恒等的に $\Phi_{\boldsymbol{v}} = 0$ であるための必要十分条件は $\boldsymbol{v} = \boldsymbol{0}$ である．

2. $\boldsymbol{v} = \boldsymbol{e}_i$ または $\boldsymbol{v} = \boldsymbol{e}_i + \boldsymbol{e}_j$ $(i \neq j)$ ならば，$\Phi_{\boldsymbol{v}} = 1$.

命題 7. m を自然数とし，$\boldsymbol{P} = (P_1, \ldots, P_n) \in J^n$, $\boldsymbol{v} \in \mathbb{Z}^m$ とする．$T = (t_{ij})$ を整数成分の $n \times m$ 行列とする．このとき次の式が成り立つ．

$$\Phi_{\boldsymbol{v}}(\boldsymbol{P}T) = \frac{\Phi_{T\boldsymbol{v}}(\boldsymbol{P})}{\prod_{i=1}^{m} \Phi_{T\boldsymbol{e}_i}(\boldsymbol{P})^{2v_i^2 - \sum_{j=1}^{m} v_i v_j} \prod_{1 \leq i < j \leq m} \Phi_{T(\boldsymbol{e}_i + \boldsymbol{e}_j)}(\boldsymbol{P})^{v_i v_j}},$$

ここで，$\boldsymbol{P}T = ([t_{11}]P_1 + \cdots + [t_{n1}]P_n, \ldots, [t_{1m}]P_1 + \cdots + [t_{nm}]P_n)$ とする．

$J \times J$ 上の有理関数 $\mathcal{F}_g$ を $\mathcal{F}_g(P,Q) = \Phi_{(1,-1)}(P,Q)$ で定義する．$\Phi_{\boldsymbol{v}}$ の定義から，

$$\Phi_{(1,-1)}(u,v) = \frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2}$$

であり，これを Weierstrass の $\wp$ 関数の拡張を用いて書き表す公式が知られている (cf. [3])．命題 7 から次の命題が従う．

命題 8. $\boldsymbol{P} = (P_1, \ldots, P_n) \in J^n$, $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{Z}^n$ とする．$\boldsymbol{v}, \boldsymbol{w}, \boldsymbol{v}+\boldsymbol{w}, \boldsymbol{v}-\boldsymbol{w} \neq \boldsymbol{0}$ ならば，次の式が成り立つ．

$$\frac{\Phi_{\boldsymbol{v}+\boldsymbol{w}}(\boldsymbol{P})\Phi_{\boldsymbol{v}-\boldsymbol{w}}(\boldsymbol{P})}{\Phi_{\boldsymbol{v}}(\boldsymbol{P})^2\Phi_{\boldsymbol{w}}(\boldsymbol{P})^2} = \mathcal{F}_g([v_1]P_1 + \cdots + [v_n]P_n, [w_1]P_1 + \cdots + [w_n]P_n).$$

$\Phi_{\boldsymbol{v}}$ に関する漸化式は次のように与えられる．

定理 9. $m > 2^g$ を整数とし，$1 \leq i \leq m$ に対して $\boldsymbol{v}^{(i)} \in ((1/2)\mathbb{Z})^n$ であるとする．すべての $1 \leq i, j \leq m$ に対して $\boldsymbol{v}^{(i)} + \boldsymbol{v}^{(j)}, \boldsymbol{v}^{(i)} - \boldsymbol{v}^{(j)} \in \mathbb{Z}^n$ であると仮定する．m 次正方行列 A を

$$A = \left(\Phi_{\boldsymbol{v}^{(i)}+\boldsymbol{v}^{(j)}}\Phi_{\boldsymbol{v}^{(i)}-\boldsymbol{v}^{(j)}}\right)_{1 \leq i,j \leq m}$$

で定義する．このとき，$\det A = 0$ である．特に，$g \equiv 1,2 \pmod 4$ かつ m が偶数ならば，A は交代行列であり，$\mathrm{pf}\, A = 0$ である．ただし，$\mathrm{pf}\, A$ は A の Pfaffian である．

ここまで複素数体上で考えていたが，楕円曲線の場合と同様に任意の体 K 上で考えることができる．実際，K 上で定義された超楕円曲線 C に対して，C の Jacobi 多様体を J とすると，J^n 上の有理関数 $\Phi_{\boldsymbol{v}}$ が定義されて，ここまで述べた性質を満たしている．

超楕円曲線に対応する hyperelliptic net は次のように定義される．

定義 10. $P_1, \ldots, P_n \in J(K)$ とする．すべての $1 \leq i \leq n$ に対して $P_i \notin \Theta$ であり，すべての $1 \leq i < j \leq n$ に対して $P_i + P_j \notin \Theta$ であると仮定する．このとき，写像 $W_{P_1,\ldots,P_n} : \mathbb{Z}^n \to K$ を

$$W_{P_1,\ldots,P_n}(\boldsymbol{v}) = \Phi_{\boldsymbol{v}}(P_1, \ldots, P_n)$$

で定義し，C, P_1, …, P_n に対応する **hyperelliptic net** と呼ぶ．

5 Tate-Lichtenbaum ペアリング

本節では，hyperelliptic net を用いて超楕円曲線上の Tate-Lichtenbaum ペアリングを書き表せることを示す．

まず Tate-Lichtenbaum ペアリングについて述べる．C を $\mathbb{F}_q$ 上定義された既約非特異射影代数曲線とし，少なくとも 1 つ $\mathbb{F}_q$ 有理点を持つとする．C の $\mathbb{F}_q$ 上定義された次数 0 の因子類全体がなす群を $\mathrm{Pic}^0(C)$ とする．m を $q-1$ の正の約数とする．

C 上の Tate-Lichtenbaum ペアリング

$$\tau_m : \mathrm{Pic}^0(C)[m] \times \mathrm{Pic}^0(C)/m\,\mathrm{Pic}^0(C) \to \mathbb{F}_q^{\times}/(\mathbb{F}_q^{\times})^m$$

を次のように定義する．$\overline{D} \in \mathrm{Pic}^0(C)[m]$, $\overline{E} \in \mathrm{Pic}^0(C)$ とする．D, E をそれぞれ $\overline{D}, \overline{E}$ の代表元として，D と E は共通の点を持たないと仮定する．$mD \sim 0$ となるから，$\mathbb{F}_q$ 上定義された C 上の有理関数 f_D で $\mathrm{div}(f_D) = mD$ となるものが存在する．$E = \sum_{i=1}^{r} n_i(Q_i)$, $n_i \in \mathbb{Z}$, $Q_i \in C(\overline{\mathbb{F}}_q)$ として，

$$\tau_m(\overline{D}, \overline{E}) = \prod_{i=1}^{r} f_D(Q_i)^{n_i} \bmod (\mathbb{F}_q^{\times})^m$$

と定義する．

Tate-Lichtenbaum ペアリング τ_m は，双線形かつ非退化である．Frey-Rück [4] による非退化性の証明は，Tate [14] と Lichtenbaum [6] の結果に基づくものである．より直接的な証明が，[1, 5, 10] で与えられている．

J を C の Jacobi 多様体とする．群同型 $\lambda\colon \mathrm{Pic}^0(C) \to J(\mathbb{F}_q)$ によって τ_m を双線形写像

$$J(\mathbb{F}_q)[m] \times J(\mathbb{F}_q)/mJ(\mathbb{F}_q) \to \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^m$$

と見なすことができる．

以下，$\mathbb{F}_q$ 上定義された種数 g の超楕円曲線

$$C\colon y^2 + (b_g x^g + \cdots + b_0)y = x^{2g+1} + a_{2g}x^{2g} + \cdots + a_0$$

を考える．これはただ1つの無限遠点 $\infty \in C(\mathbb{F}_q)$ を持つ．楕円曲線の場合と同様に，hyperelliptic net を用いて Tate-Lichtenbaum ペアリングは次のように表される．

定理 11. $P \in J(\mathbb{F}_q)[m]$, $Q \in J(\mathbb{F}_q)$, $P, Q, P+Q \notin \Theta$ であると仮定する．このとき，

$$\tau_m(P,Q) = \frac{W_{P,Q}(m+1,1)W_{P,Q}(1,0)}{W_{P,Q}(m+1,0)W_{P,Q}(1,1)} \bmod (\mathbb{F}_q^\times)^m.$$

6 ペアリングの計算アルゴリズム

Stange は elliptic net を高速に計算するアルゴリズムを考案し，楕円曲線上の Tate ペアリングが $O(\log m)$ 回の四則演算で計算できることを示した．種数2の超楕円曲線についてもこのアルゴリズムを拡張して，Tate-Lichtenbaum ペアリングを $O(\log m)$ 回の四則演算で計算できることを以下に示す．

以下，前節と同じ記号を用い，$g = 2$ であるとする．すなわち，次のような超楕円曲線を考える．

$$C\colon y^2 + (b_2x^2 + b_1x + b_0)y = x^5 + a_4x^4 + \cdots + a_0.$$

簡単のため，$W_{P,Q}(m,n)$ を $W(m,n)$ と表す．

定理11によれば，$W(m,0), W(m,1)$ を計算するアルゴリズムを構成すれば十分である．そのようなアルゴリズムは Stange が与えたアルゴリズムを拡張して得られる．

整数 k に対し，k を中心とするブロック V を

$$V = [[W(k-7,0), W(k-6,0), \ldots, W(k+8,0)],\\ [W(k-3,1), W(k-2,1), \ldots, W(k+3,1)]]$$

で定義する．このブロック V を引数とする，次の二つの関数を定義する．

1. Double(V): $2k$ を中心とするブロックを返す.

2. DoubleAdd(V): $2k+1$ を中心とするブロックを返す.

これらの関数で返されるブロックは，hyperelliptic net が満たす漸化式（定理 9）を用いて計算される．これについてより詳しく述べる．

定理 9 において，$g=2, m=6$ とすると，行列

$$A = \left(W(\boldsymbol{v}^{(i)}+\boldsymbol{v}^{(j)})W(\boldsymbol{v}^{(i)}-\boldsymbol{v}^{(j)})\right)_{1\le i,j\le 6}$$

に対して，$\operatorname{pf} A = 0$ が成り立つ．$\boldsymbol{v}^{(i)} = (m_i, n_i)$ とおいて，Pfaffian の展開公式を用いると，

$$\sum_{i=2}^{6}(-1)^i \operatorname{pf} A^{1,i} \cdot W(m_1+m_i, n_1+n_i)W(m_1-m_i, n_1-n_i) = 0$$

となる．ここで，$A^{1,i}$ は A の第 1 行，第 i 行，第 1 列，第 i 列を取り除いて得られる 4 次正方行列である．この式において，m_i, n_i の値を表 1 のように定めることで，Double(V), DoubleAdd(V) を計算する漸化式が得られる．ただし，$-3 \le j \le 4$ とする．

	m_1	m_2	m_3	m_4	m_5	m_6	n_1	$n_2, \ldots, n_6$
$W(2k,0)$	$k+1$	$k-1$	3	2	1	0	0	0
$W(2k-1,0)$	k	$k-1$	3	2	1	0	0	0
$W(2k+j,1)$	k	$k+j$	3	2	1	0	1	0

表 1: m_i と n_i の値

漸化式の計算の際に，$W(m_1-m_2, n_1-n_2)\operatorname{pf} A^{1,2}$ による除算が必要である．しかし，これらは j, k に依存しないので，逆数をあらかじめ計算しておけば，除算を避けることができる．$\operatorname{pf} A^{1,2}$ は P のみによって定まる値なので，$\Delta(P)$ と表すことにする．すなわち，

$$\Delta(P) = \operatorname{pf} A^{1,2} = W(5,0) - W(4,0)W(2,0)^3 + W(3,0)^3.$$

以上から，$W(m,0)$ と $W(m,1)$ を求めるアルゴリズムは Algorithm 1 のように書ける．

Algorithm 1 Hyperelliptic Net Algorithm

Input: Hyperelliptic net の初期値 $W(i,0)$ $(-6 \leq i \leq 9)$, $W(i,1)$ $(-4 \leq i \leq 4)$ と整数 m. m の 2 進展開を $m = (d_k d_{k-1} \ldots d_1)_2$ $(d_k = 1)$ とする.

Output: $W(m,0)$, $W(m,1)$

1: $V \leftarrow [[W(-6,0), W(-5,0), \ldots, W(9,0)],$
$[W(-2,1), W(-1,1), \ldots, W(4,1)]]$
2: **for** $i = k-1$ down to 1 **do**
3: **if** $d_i = 0$ **then**
4: $V \leftarrow \mathrm{Double}(V)$
5: **else**
6: $V \leftarrow \mathrm{DoubleAdd}(V)$
7: **end if**
8: **end for**
9: **return** $V[0,7]$, $V[1,3]$ // $W(m,0)$, $W(m,1)$

Algorithm 1 では初期値 $W(i,0)$ $(-6 \leq i \leq 9)$, $W(i,1)$ $(-4 \leq i \leq 4)$ の計算をあらかじめしておく必要がある. この初期値は次のように計算される. $P, Q \in J(\mathbb{F}_q)$ の Mumford 表現をそれぞれ $(t^2 + u_{11}t + u_{12}, v_{11}t + v_{12})$, $(t^2 + u_{21}t + u_{22}, v_{21}t + v_{22})$ とする. 言い換えれば, 点 P が因子 $(x_1, y_1) + (x_2, y_2) - 2(\infty)$ に対応するとき,

$$u_{11} = -(x_1 + x_2), \qquad u_{12} = x_1 x_2,$$
$$v_{11} = \frac{y_1 - y_2}{x_1 - x_2}, \qquad v_{12} = \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2}$$

である. 点 Q についても同様である. まず, $W(0,0)$, $W(1,0)$, $W(0,1)$, $W(1,1)$, $W(2,0)$ の値を次の式で計算する.

$$W(0,0) = 0, \quad W(1,0) = W(0,1) = W(1,1) = 1,$$
$$\begin{aligned} W(2,0) = {} & (-4u_{12} + 6{u_{11}}^2 + (-{b_2}^2 - 4a_4)u_{11} + b_1 b_2 + 2a_3)v_{12} + 2{v_{11}}^3 \\ & + (3b_1 - 3b_2 u_{11}){v_{11}}^2 + ((-8u_{11} + {b_2}^2 + 4a_4)u_{12} + 2{u_{11}}^3 \\ & + ({b_2}^2 - 2a_4){u_{11}}^2 + (2a_3 - 2b_1 b_2)u_{11} - b_0 b_2 + {b_1}^2 - 2a_2)v_{11} \\ & + 2b_2 {u_{12}}^2 + (b_2 {u_{11}}^2 - 4b_1 u_{11} - a_3 b_2 + 2a_4 b_1 - 2b_0)u_{12} \\ & - b_2 {u_{11}}^4 + (a_4 b_2 + b_1){u_{11}}^3 + (-a_3 b_2 - a_4 b_1 + 3b_0){u_{11}}^2 \\ & + (a_2 b_2 + a_3 b_1 - 2a_4 b_0)u_{11} - a_2 b_1 + a_3 b_0. \end{aligned}$$

他の項は，直接計算するには式が巨大すぎるので，命題8から得られる次の公式を用いる．

$$\frac{W(m+1,i)W(m-1,i)}{W(m,i)^2} = \mathcal{F}_2([m]P+[i]Q,P) \tag{1}$$

ここで，$i=0,1$ であり，$\mathcal{F}_2(P,Q)$ は次の式で計算される．

$$\mathcal{F}_2(P,Q) = -(v_{11}^2 - b_2u_{11}v_{11} + b_1v_{11} - u_{11}u_{12} + u_{11}^3 - a_4u_{11}^2 + a_3u_{11})$$
$$+(v_{21}^2 - b_2u_{21}v_{21} + b_1v_{21} - u_{21}u_{22} + u_{21}^3 - a_4u_{21}^2 + a_3u_{21}) - u_{12}u_{21} + u_{11}u_{22}.$$

式 (1) で $W(m+1,i)$ を計算する際に $W(m-1,i)$ による除算が必要であることに注意しなければならない．

以上のアルゴリズムによって，次の定理が得られる．

定理 12. 次の値がすべて0でないと仮定する．

$$W(2,0), W(3,0), \ldots, W(8,0),$$
$$W(-4,1), W(-3,1), \ldots, W(3,1), \Delta(P). \tag{2}$$

このとき，$W(m,0)$ と $W(m,1)$ は $\mathbb{F}_q$ における $O(\log m)$ 回の四則演算で計算できる．

定理11を用いると，次の系を得る．

系 13. (2) の値がすべて0でないならば，$\tau_m(P,Q)$ は $\mathbb{F}_q$ における $O(\log m)$ 回の四則演算で計算できる．

注意 14. Miller のアルゴリズムを用いた場合も，$\tau_m(P,Q)$ を $\mathbb{F}_q$ における $O(\log m)$ 回の四則演算で計算できる．

本節で述べたアルゴリズムは，次のような特徴を持つ．

- $\mathbb{F}_q$ における除算をほとんど必要としない．より正確に言えば，除算回数は m に依存しない．
- Miller のアルゴリズムとは異なり，計算時間が m の Hamming 重み（2進展開における1の個数）にほとんど依存しない．
- $\mathbb{F}_q$ の拡大体における計算を必要としない．

7 まとめ

本稿では，Stangeによって定義されたelliptic netを超楕円曲線に拡張し，hyperelliptic netを定義した．また，hyperelliptic netが満たす漸化式を導いた．次に，超楕円曲線上のTate-Lichtenbaumペアリングをhyperelliptic netで表す公式を述べた．最後に，hyperelliptic netを用いて種数2の超楕円曲線上のTate-Lichtenbaumペアリングを計算するアルゴリズムを与えた．

Hyperelliptic netを用いたアルゴリズムの実装については，田中覚氏（首都大学東京）との共同研究[13]により行われている．この結果によれば，実用的な曲線について実装評価は得られたものの，Millerのアルゴリズムと比較してまだ改善の余地がかなりあると考えられる．Elliptic netの計算で行われているような，演算量の削減による高速化が今後の課題である．

参考文献

[1] P. Bruin, "The Tate pairing for Abelian varieties over finite fields," J. Théor. Nombres Bordeaux **23** (2011) 323–328.

[2] V. M. Buchstaber, V. Z. Enolskii, D. V. Leykin, "Kleinian functions, hyperelliptic Jacobians and applications," Rev. Math. Math. Phys. **10** (1997) 1–125.

[3] V. M. Buchstaber, V. Z. Enolskii, D. V. Leykin, "A recursive family of differential polynomials generated by the Sylvester identity and addition theorems for hyperelliptic Kleinian functions," Funct. Anal. Appl. **31** (1997) 240–251.

[4] G. Frey, H.-G. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves," Math. Comp. **62** (1994) 865–874.

[5] F. Hess, "A note on the Tate pairing of curves over finite fields," Arch. Math. (Basel) **82** (2004), 28–32.

[6] S. Lichtenbaum, "Duality theorems for curves over p-adic fields," Invent. Math. **7** (1969) 120–136.

[7] V. S. Miller, "Short programs for functions on curves," unpublished manuscript (1986), `http://crypto.stanford.edu/miller/`.

[8] V. S. Miller, "The Weil pairing, and its efficient calculation," J. Cryptology **17** (2004) 235–261.

[9] 大西良博, "超楕円函数論," 第 15 回整数論サマースクール報告集 (2008) 131–176, `http://www.ccn.yamanashi.ac.jp/~yonishi/ /research/pub/ss2007/06onishi.pdf`.

[10] E. F. Schaefer, "A new proof for the non-degeneracy of the Frey-Rück pairing and a connection to isogenies over the base field," *Computational aspects of algebraic curves*, 1–12, Lecture Notes Ser. Comput. 13, World Sci. Publ., Hackensack, NJ, 2005.

[11] K. E. Stange, "The Tate pairing via elliptic nets," *Pairing-Based Cryptography—Pairing 2007*, 329–348, Lecture Notes in Comput. Sci., 4575, Springer, Berlin, 2007.

[12] K. E. Stange, "Elliptic nets and elliptic curves," Algebra Number Theory **5** (2011) 197–229.

[13] 田中覚, 内田幸寛, 内山成憲, "Hyperelliptic Net を用いた Tate-Lichtenbaum Pairing の実装について," 日本応用数理学会 2012 年度講演予稿集 (2012) 19–20.

[14] J. Tate, "WC-groups over $\mathfrak{p}$-adic fields," Séminaire Bourbaki, exp. no. 156 (1957).

[15] Y. Uchida, S. Uchiyama, "The Tate-Lichtenbaum pairing on a hyperelliptic curve via hyperelliptic nets," *Pairing-Based Cryptography—Pairing 2012*, 218–233, Lecture Notes in Comput. Sci., 7708, Springer, Berlin, 2013.

[16] M. Ward, "Memoir on elliptic divisibility sequences," Amer. J. Math. **70** (1948) 31–74.